contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Synology DiskStation Manager (DSM) exploited

CVE-2024-10441 · on CISA's exploited list since 18 November 2026

Analysis Report

Anyone running a Synology DiskStation (DSM) or BeeStation must update by 21 November 2026, CISA's date. First, read the version on each device and compare it with the fixed versions below. If you run …

PREPARED BY	NamiQ	DATE	18 November 2026
FACTS AS OF	18 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 21 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/synology-diskstation-manager-dsm-cve-2024-10441

The bottom line

> *Anyone running a Synology DiskStation (DSM) or BeeStation must update by 21 November 2026, CISA's date. First, read the version on each device and compare it with the fixed versions below. If you run no Synology device, you can stop here.*

At a glance

Fact	Detail
Product	Synology DiskStation Manager (DSM) (CVE-2024-10441)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 18 November 2026. Deadline for US federal agencies: 21 November 2026.
Chance of exploitation (EPSS)	0.01, the estimated chance in the next 30 days, as at 18 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	DSM 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4, 7.1.1-42962-7; BSM 1.1-65374 (vendor advisory, first published 5 November 2024)
Who looks first	Anyone with a DiskStation on DSM 7.1, 7.2, 7.2.1 or 7.2.2, or a BeeStation on BSM 1.0 or 1.1, below the fixed version. Devices reachable from the internet come first.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run a Synology DiskStation (DSM) or BeeStation (BSM)?	Nothing to do for this CVE.	Check the version (next question).
Is it DSM 7.1, 7.2, 7.2.1 or 7.2.2, or BeeStation OS 1.0 or 1.1?	The record does not list your version. Nothing more for this CVE.	Compare it with the fixed version (next question).
Is the version below the fixed one, such as DSM 7.2.2 older than 7.2.2-72806-1?	You are on or above the fixed version. Note the version and stop.	Update it. Ask next whether it is exposed.

Can the device be reached from the internet, or by anyone you do not trust?	Still update, but it is less urgent than an exposed device.	Treat it as urgent: update before 21 November 2026.

What it is

The record says a flaw in the system plugin daemon lets a remote attacker run their own code on the device. The score vector says no login and no user action are needed. How it is reached is not published ("unspecified vectors").

Why it matters

Our reading is that a remote code-execution flaw needing no login gives an attacker a foothold on a device inside your network, and from there they can run what they like on it. The vendor's advisory says there is no mitigation, so updating is the only listed fix. The same advisory fixes two lower-scored flaws in the same release, so one update closes all three.

What the vendor's advisory says

We read three pages on www.synology.com. In short:

- Synology's advisory (first published 5 November 2024) fixes three flaws together: CVE-2024-10441 (9.8), CVE-2024-50629 (5.3) and CVE-2024-10445 (4.3).
- The advisory says CVE-2024-50629 lets remote attackers read limited files. It says CVE-2024-10445 lets attackers write limited files through the update function, from an adjacent network position.
- The advisory lists the mitigation as "None". Updating is the only action it names.
- The advisory also lists DSM 6.2, fixed in 6.2.4-25556-8, but only for CVE-2024-10445. The record for this CVE does not list 6.2.
- The advisory's revision notes say updates became available for DSM 7.2.1 on 12 November 2024 and for DSM 7.1 on 26 November 2024.

Things people will get wrong

- "The details are unspecified, so nobody can use it." "Unspecified vectors" means the details are not published. The score vector still says network access, low complexity, no login and no user action.
- "We run DSM 6.2, so this CVE applies to us." The record does not list DSM 6.2. The advisory lists 6.2 only for CVE-2024-10445.
- "A firewall rule or setting will do instead of updating." The advisory lists the mitigation as "None". Limiting exposure helps, but the fix is the update.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page before you run them. Words in capitals are for you to fill in.

Step 1: Find the versions you run

- List every DiskStation and BeeStation you own, including ones at home offices or branches.
- Read the DSM or BSM version on each and compare it with the fixed versions above.

```
cat /etc.defaults/VERSION
```

Step 2: Reduce exposure until it is updated

- Take the device off the internet where you can. The advisory names no workaround, so this only lowers the risk.
- Remove any port forwarding to it from the router.

Step 3: Update to the fixed version

- Move each device to the fixed version for its line, or later, as the vendor's advisory states.
- Do this before CISA's date of 21 November 2026.

Step 4: Check the result

- Read the version again and confirm it is at or above the fixed one.
- Keep the version for each device in writing.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need to confirm our exposure to CVE-2024-10441 in Synology DiskStation Manager (DSM) and BeeStation OS. Please tell us whether we run either, where, and which version each device is on. The vendor's fixed versions are DSM 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4 and 7.1.1-42962-7, and BSM 1.1-65374. CISA's date is 21 November 2026. Please update anything below those versions and confirm the versions and the update to us in writing before that date.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Unexpected processes, scheduled tasks or new accounts on the device, since arbitrary code could create them.
- A DSM or BSM version number that is not the one you last installed.
- Unexpected connections to the device from the internet in router or firewall logs, from before you updated.

The weakness behind it

The record classes this as CWE-116 (Improper Encoding or Escaping of Output).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record says remote attackers, and the score vector needs no login or user action. That would typically make it a way in through a device facing the network.

Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	The record says it allows arbitrary code execution. An attacker would likely use that to run commands or scripts on the device.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *Synology DSM contains an improper encoding or escaping of output vulnerability in the system plugin daemon in Synology BeeStation OS (BSM) that could allow a remote attacker to execute arbitrary code via unspecified vectors.*

The CVE record, published by Synology on 19 March 2025:

> *Improper encoding or escaping of output vulnerability in the system plugin daemon in Synology BeeStation OS (BSM) before 1.1-65374 and Synology DiskStation Manager (DSM) before 7.2-64570-4, 7.2.1-69057-6 and 7.2.2-72806-1 allows remote attackers to execute arbitrary code via unspecified vectors.*

Versions of Synology DiskStation Manager (DSM) the record lists as affected:

- 7.2.2 up to, but not including, 7.2.2-72806-1
- 7.2.1 up to, but not including, 7.2.1-69057-6
- 7.2 up to, but not including, 7.2-64570-4
- 7.1 up to, but not including, 7.1.1-42962-7

The affected ranges end before 7.2.2-72806-1, 7.2.1-69057-6, 7.2-64570-4, 7.1.1-42962-7. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

Versions of Synology BeeStation OS (BSM) the record lists as affected:

- 1.1 up to, but not including, 1.1-65374
- 1.0 up to, but not including, 1.1-65374

The affected ranges end before 1.1-65374. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2024-10441
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2024-10441
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The record says "unspecified vectors", so how the flaw is reached is not published.
- No source says which network service of the system plugin daemon an attacker would reach.
- No source says how attackers have used it, or what they did after getting access.
- No source names any workaround; the advisory lists the mitigation as "None".

- We have not tested this against any environment. Versions and scores are as the sources state them and as at 18 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2024-10441: score 9.8, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
19 March 2025	CVE record published by Synology.
18 November 2026	CISA added it to its list of exploited vulnerabilities.
21 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
A DSM or BSM device below the fixed version, reachable from the internet	High	Within CISA's window
A device below the fixed version, reachable only from inside your network	Medium	This week
You do not know which version your Synology devices run	Medium	Find out today

DSM 6.2 only; the record for this CVE does not list it	Low	Next patch cycle
A device already on or above the fixed version	None	None for this CVE

Appendix 4. Definition of done

- Every Synology DiskStation Manager (DSM) you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2024-10441: https://www.cve.org/CVERecord?id=CVE-2024-10441
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: www.synology.com/en-global/security/advisory/Synology_SA_24_20: https://www.synology.com/en-global/security/advisory/Synology_SA_24_20
- Advisory or release notes read: www.synology.com/en-global/security/advisory/Synology_SA_24_23: https://www.synology.com/en-global/security/advisory/Synology_SA_24_23
- Advisory or release notes read: www.synology.com/zh-tw/security/advisory/Synology_SA_24_20: https://www.synology.com/zh-tw/security/advisory/Synology_SA_24_20